

SON-2356

PATENT APPLICATION

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re the Patent Application of)

Akira Kimura)

Serial No.: (Not yet assigned))

Filed: February 26, 2002)

ATTN: APPLICATION BRANCH

For: AUTHENTICATION SYSTEM AND METHOD, IDENTIFICATION INFORMATION
INPUTTING METHOD AND APPARATUS AND PORTABLE TERMINAL

CLAIM TO PRIORITY UNDER 35 U.S.C. 119

Assistant Commissioner for Patents
Washington, D.C. 20231

Sir:

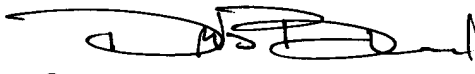
The benefit of the filing date of the following prior applications filed in the following foreign country is hereby requested and the right of priority provided under 35 U.S.C. 119 is hereby claimed:

Japanese Patent Application 2001-052770, filed February 27, 2001.

In support of this claim, filed herewith are certified copies of said original foreign applications.

Respectfully submitted,

Dated: February 26, 2002


Ronald P. Kananen
Reg. No. 24,104

RADER, FISHMAN & GRAUER P.L.L.C.
1233 20TH Street, N.W., Suite 501
Washington, DC 20036
Telephone: (202) 955-3750
Facsimile: (202) 955-3751
Customer No.: 23353



日 本 国 特 許 庁
JAPAN PATENT OFFICE

1c879 U.S. PTC
10/082186
02/26/03

別紙添付の書類に記載されている事項は下記の出願書類に記載されて
いる事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed
with this Office

出 願 年 月 日
Date of Application:

2001年 2月27日

出 願 番 号
Application Number:

特願2001-052770

ST.10/C]:

[JP2001-052770]

出 願 人
Applicant(s):

ソニー株式会社

CERTIFIED COPY OF
PRIORITY DOCUMENT

2002年 2月 1日

特 許 庁 長 官
Commissioner,
Japan Patent Office

及 川 耕 造



出証番号 出証特2002-3002952

【書類名】 特許願

【整理番号】 0000963406

【提出日】 平成13年 2月27日

【あて先】 特許庁長官 及川 耕造 殿

【国際特許分類】 G06F 17/60

【発明者】

【住所又は居所】 東京都品川区北品川6丁目7番35号 ソニー株式会社
内

【氏名】 木村 明

【特許出願人】

【識別番号】 000002185

【氏名又は名称】 ソニー株式会社

【代理人】

【識別番号】 100067736

【弁理士】

【氏名又は名称】 小池 晃

【選任した代理人】

【識別番号】 100086335

【弁理士】

【氏名又は名称】 田村 榮一

【選任した代理人】

【識別番号】 100096677

【弁理士】

【氏名又は名称】 伊賀 誠司

【手数料の表示】

【予納台帳番号】 019530

【納付金額】 21,000円

【提出物件の目録】

【物件名】 明細書 1

【物件名】 図面 1

【物件名】 要約書 1

【包括委任状番号】 9707387

【プルーフの要否】 要

【書類名】 明細書

【発明の名称】 認証システム及び認証方法、並びに暗号入力装置及び暗号入力方法、並びに携帯端末

【特許請求の範囲】

【請求項 1】 携帯端末と上記携帯端末とは独立して設けられ上記携帯端末との間で通信する認証装置とから構成される認証システムにおいて、

上記携帯端末は、

上記携帯端末を識別するための第 1 の識別情報が予め記憶された第 1 の識別情報記憶手段と、

上記第 1 の識別情報に対応付けられた第 2 の識別情報を入力するための操作手段と、

上記操作手段によって入力された第 2 の識別情報を所定の暗号生成情報に基づいて暗号化する暗号化手段と、

上記認証装置との通信を行う第 1 の通信手段と

を備え、

上記認証装置は、

上記第 1 の識別情報と上記第 2 の識別情報とが記憶される第 2 の識別情報記憶手段と、

上記暗号生成情報を発生する暗号生成情報発生手段と、

上記携帯端末との通信を行う第 2 の通信手段と、

上記暗号化手段によって暗号化された上記第 2 の識別情報を上記暗号生成情報に基づいて比較し認証する比較認証手段と

を備え、

該携帯端末において、上記操作手段により入力された第 2 の識別情報を上記第 1 の通信手段を介して上記認証装置から受信した上記暗号生成情報に基づいて暗号化し、上記暗号化された第 2 の識別情報を上記第 1 の通信手段を介して上記認証装置に送信し、該認証装置において、上記第 2 の通信手段を介して受信した上記暗号化された第 2 の識別情報と上記第 2 の識別情報記憶手段に記憶された第 2 の識別情報とを上記暗号生成情報に基づいて比較し認証することを特徴とする認

証システム。

【請求項 2】 上記認証装置は、

上記暗号化手段によって暗号化された第 2 の識別情報を上記暗号生成情報に基づいて復号する復号手段を備え、

上記認証装置は、受信した上記暗号化された第 2 の識別情報を上記暗号生成情報に基づいて復号し、上記復号された第 2 の識別情報と上記第 2 の識別情報記憶手段に記憶された第 2 の識別情報とを比較して認証することを特徴とする請求項 1 記載の認証システム。

【請求項 3】 上記暗号生成情報は、所定の文字数の乱数であることを特徴とする請求項 2 記載の認証システム。

【請求項 4】 所定のネットワークを介して行われる信用販売制度、口座間即時決済及び電子商取引において、サービス提供者が所定のサービスを提供するサービス利用者を認証するための認証システムであって、

上記携帯端末は、上記サービス提供者が上記サービス利用者に対して発行するカード形状を呈する携帯端末であり、

上記認証装置は、上記サービス提供者が上記サービス利用者の利用情報を認証するためのホストコンピュータに含まれる認証装置であり、

上記カード形状の携帯端末とこの携帯端末の所有者が真の所有者であることとを認証することによって、上記サービス利用者を認証することを特徴とする請求項 3 記載の認証システム。

【請求項 5】 上記第 1 の通信手段及び上記第 2 の通信手段は、有線通信手段又は無線通信手段であることを特徴とする請求項 4 記載の認証システム。

【請求項 6】 上記携帯端末は、上記第 2 の識別情報が記憶される一時記憶手段を備えることを特徴とする請求項 4 記載の認証システム。

【請求項 7】 上記一時記憶手段には、上記認証装置が上記携帯端末を認証するまで上記操作手段において入力された第 2 の識別情報が記憶されることを特徴とする請求項 4 記載の認証システム。

【請求項 8】 上記一時記憶手段に記憶された第 2 の識別情報は、所定時間毎に消去されることを特徴とする請求項 4 記載の認証システム。

【請求項 9】 上記携帯端末において、上記操作手段は、上記一時記憶手段に記憶された第 2 の識別情報を消去する手段を含むことを特徴とする請求項 4 記載の認証システム。

【請求項 1 0】 上記携帯端末において、上記操作手段は、上記第 2 の識別情報を入力するための複数の文字入力部を備え、上記文字入力部の配置位置が可変とされていることを特徴とする請求項 4 記載の認証システム。

【請求項 1 1】 上記文字入力部の配置位置は、上記第 2 の識別情報の入力前に変化することを特徴とする請求項 1 0 記載の認証システム。

【請求項 1 2】 上記携帯端末において、上記操作手段は、文字を表示する表示部と上記表示部に表示された文字を選択するための選択部とを備え、上記操作手段において入力される第 2 の識別情報は、上記表示部に次々に表示された複数の文字の中から上記選択部により選択された文字列で構成されることを特徴とする請求項 1 0 記載の認証システム。

【請求項 1 3】 携帯端末とこの携帯端末とは独立して設けられた認証装置との間で上記認証装置が上記携帯端末を認証する認証方法において、

第 1 の識別情報記憶手段に予め記憶された上記携帯端末を識別するための第 1 の識別情報に対応付けられた第 2 の識別情報を入力する操作工程と、

暗号生成情報を発生する暗号生成情報発生工程と、

上記操作工程において入力された第 2 の識別情報を上記暗号生成情報発生工程において発生された暗号生成情報に基づいて暗号化する暗号化工程と、

上記暗号化工程において暗号化された第 2 の識別情報を上記暗号生成情報に基づいて比較し認証する比較認証工程と

を備えることを特徴とする認証方法。

【請求項 1 4】 上記暗号化工程において暗号化された第 2 の識別情報を上記暗号生成情報に基づいて復号する復号工程を備え、

上記暗号化された第 2 の識別情報を上記復号工程において上記暗号生成情報に基づいて復号し、上記復号された第 2 の識別情報と第 2 の識別情報記憶手段に記憶された第 2 の識別情報とを比較して認証することを特徴とする請求項 1 3 記載の認証方法。

【請求項 1 5】 上記暗号生成情報は、所定の文字数の乱数であることを特徴とする請求項 1 4 記載の認証方法。

【請求項 1 6】 所定のネットワークを介して行われる信用販売制度、口座間即時決済及び電子商取引において、サービス提供者が所定のサービスを提供するサービス利用者を認証するための認証方法であって、

上記携帯端末は、上記サービス提供者が上記サービス利用者に対して発行するカード形状を呈する携帯端末であり、

上記認証装置は、上記サービス提供者が上記サービス利用者の利用情報を認証するためのホストコンピュータに含まれる認証装置であり、

上記カード形状の携帯端末とこの携帯端末の所有者が真の所有者であることとを認証することによって、上記サービス利用者を認証することを特徴とする請求項 1 5 記載の認証方法。

【請求項 1 7】 上記携帯端末と上記認証装置との間は、有線通信手段又は無線通信によって接続されることを特徴とする請求項 1 6 記載の認証方法。

【請求項 1 8】 上記携帯端末は、上記第 2 の識別情報を一時記憶手段に一時的に記憶する一時記憶工程を備えることを特徴とする請求項 1 6 記載の認証方法。

【請求項 1 9】 上記一時記憶工程では、上記認証装置が上記携帯端末を認証するまで上記操作工程において入力された第 2 の識別情報を記憶することを特徴とする請求項 1 6 記載の認証方法。

【請求項 2 0】 上記一時記憶工程で記憶された第 2 の識別情報は、所定時間毎に消去されることを特徴とする請求項 1 6 記載の認証方法。

【請求項 2 1】 上記操作工程には、上記第 2 の認証情報記憶手段に記憶された第 2 の識別情報を消去する工程が含まれることを特徴とする請求項 1 6 記載の認証方法。

【請求項 2 2】 上記操作工程には、上記第 2 の識別情報を入力するための文字入力工程が含まれ、上記文字入力工程では、配置が可変とされた複数の文字入力部によって上記第 2 の識別情報が入力されることを特徴とする請求項 1 6 記載の認証方法。

【請求項 2 3】 上記文字入力工程において、複数の文字の配置は、上記第 2 の識別情報が入力される前に変更されることを特徴とする請求項 2 2 記載の認証方法。

【請求項 2 4】 上記操作工程には、文字を表示する表示工程と上記表示工程において表示された文字を選択するための選択工程とが含まれ、上記操作工程において入力される第 2 の識別情報は、上記表示工程において次々に表示された複数の文字の中から上記選択工程において選択された文字列で構成されることを特徴とする請求項 2 2 記載の認証方法。

【請求項 2 5】 所定の文字群に含まれる文字の組み合わせから構成される所定数の文字列を認証用文字列とする暗号入力装置において、

上記所定の文字群に含まれる文字を不規則に表示する表示手段と、

上記表示手段に不規則に表示される文字のなかから上記認証用文字列を構成する文字を選択するための選択手段と

を備えることを特徴とする暗号入力装置。

【請求項 2 6】 上記所定の文字群は、0 から 9 で表される 1 0 個の数字であることを特徴とする請求項 2 5 記載の暗号入力装置。

【請求項 2 7】 上記表示手段は、上記数字の各々を該表示手段の任意の位置に不規則に表示することを特徴とする請求項 2 5 記載の暗号入力装置。

【請求項 2 8】 上記表示手段は、上記数字の各々を不規則な順番でひとつひとつ表示することを特徴とする請求項 2 5 記載の暗号入力装置。

【請求項 2 9】 上記表示手段は、予め記された上記 0 から 9 の数字若しくはこの数字の近傍を発光させることで各々の数字を指し示すことを特徴とする請求項 2 5 記載の暗号入力装置。

【請求項 3 0】 所定の文字群に含まれる文字の組み合わせから構成される所定数の文字列を認証用文字列とする暗号入力方法において、

上記所定の文字群に含まれる文字を不規則に表示する表示工程と、

上記表示工程において不規則に表示される文字のなかから上記認証用文字列を構成する文字を選択する選択工程と

を備えることを特徴とする暗号入力方法。

【請求項 3 1】 上記所定の文字群は、0 から 9 で表される 1 0 個の数字であることを特徴とする請求項 3 0 記載の暗号入力方法。

【請求項 3 2】 上記表示工程では、上記数字の各々を表示手段の任意の位置に不規則に表示することを特徴とする請求項 3 0 記載の暗号入力方法。

【請求項 3 3】 上記表示工程では、上記数字の各々を不規則な順番でひとつひとつ表示することを特徴とする請求項 3 0 記載の暗号入力方法。

【請求項 3 4】 上記表示工程では、予め記された上記 0 から 9 の数字若しくは上記数字の近傍を発光させることで各々の数字を指し示すことを特徴とする請求項 3 0 記載の暗号入力方法。

【請求項 3 5】 認証装置によって認証される携帯端末において、

上記携帯端末を識別するための第 1 の識別情報が予め記憶された第 1 の識別情報記憶手段と、

上記第 1 の識別情報に対応付けられた第 2 の識別情報を入力するための操作手段と、

上記認証装置との通信を行う通信手段と、

上記操作手段によって入力された第 2 の識別情報を上記通信手段を介して上記認証装置から送られる所定の暗号生成情報に基づいて暗号化する暗号化手段と

を備えることを特徴とする携帯端末。

【請求項 3 6】 上記暗号生成情報は、所定の文字数の乱数であることを特徴とする請求項 3 5 記載の携帯端末。

【請求項 3 7】 所定のネットワークを介して行われる信用販売制度、口座間即時決済及び電子商取引において、サービス提供者が所定のサービスを提供するサービス利用者を認証するために上記サービス利用者に対して発行され、カード形状を呈することを特徴とする請求項 3 5 記載の携帯端末。

【請求項 3 8】 上記通信手段は、有線通信手段又は無線通信手段であることを特徴とする請求項 3 7 記載の携帯端末。

【請求項 3 9】 上記第 2 の識別情報が記憶される一時記憶手段を備えることを特徴とする請求項 3 7 記載の携帯端末。

【請求項 4 0】 上記一時記憶手段には、上記認証装置が上記携帯端末を認証

するまで上記操作手段において入力された第 2 の識別情報が記憶されることを特徴とする請求項 3 9 記載の携帯端末。

【請求項 4 1】 上記一時記憶手段に記憶された第 2 の識別情報は、所定時間毎に消去されることを特徴とする請求項 3 9 記載の携帯端末。

【請求項 4 2】 上記操作手段は、上記一時記憶手段に記憶された第 2 の識別情報を消去する手段を含むことを特徴とする請求項 3 9 記載の携帯端末。

【請求項 4 3】 上記操作手段は、上記第 2 の識別情報を入力するための複数の文字入力部を備え、上記文字入力部の配置位置が可変とされていることを特徴とする請求項 3 7 記載の携帯端末。

【請求項 4 4】 上記文字入力部の配置位置は、上記第 2 の識別情報の入力前に変化することを特徴とする請求項 4 3 記載の携帯端末。

【請求項 4 5】 上記操作手段は、文字を表示する表示部と上記表示部に表示された文字を選択するための選択部とを備え、上記操作手段において入力される第 2 の識別情報は、上記表示部に次々に表示された複数の文字の中から上記選択部により選択された文字列で構成されることを特徴とする請求項 4 3 記載の携帯端末。

【請求項 4 6】 携帯端末と上記携帯端末とは独立して設けられ上記携帯端末との間で通信する認証装置とから構成される認証システムにおいて、

上記携帯端末は、

上記携帯端末を識別するための第 1 の識別情報が記憶された第 1 の識別情報記憶手段と、

所定の文字群に含まれる文字を不規則に表示する表示手段と、上記表示手段に不規則に表示される文字のなかから上記第 2 の識別情報を構成する文字を選択するための選択手段とを有し、上記第 1 の識別情報に対応付けられた上記第 2 の識別情報を入力するための操作手段と、

上記操作手段によって入力された第 2 の識別情報を所定の暗号生成情報に基づいて暗号化する暗号化手段と、

上記認証装置との通信を行う第 1 の通信手段とを備え、

上記認証装置は、

上記第 1 の識別情報と上記第 2 の識別情報とを記憶した第 2 の識別情報記憶手段と、

上記暗号生成情報を発生する暗号生成情報発生手段と、

上記携帯端末との通信を行う第 2 の通信手段と、

上記暗号化手段によって暗号化された第 2 の識別情報を上記暗号生成情報に基づいて比較し認証する比較認証手段と

を備え、

上記操作手段により入力された第 2 の識別情報を上記第 1 の通信手段を介して上記認証装置から受信した上記暗号生成情報に基づいて暗号化し、上記暗号化された第 2 の識別情報を上記第 1 の通信手段を介して上記認証装置に送信し、該認証装置において、上記第 2 の通信手段を介して受信した上記暗号化された第 2 の識別情報と上記第 2 の識別情報記憶手段に記憶された第 2 の識別情報とを上記暗号生成情報に基づいて比較し認証することを特徴とする認証システム。

【発明の詳細な説明】

【 0 0 0 1 】

【発明の属する技術分野】

本発明は、認証システム及び認証方法、並びに暗号入力装置及び暗号入力方法、並びに携帯端末に関し、特に、サービス提供者が利用者を認証する過程において、第三者が利用者の個人情報を不正に取得することを困難にする認証システム及び認証方法に関する。また、利用者が暗号を入力する過程において、第三者が利用者の個人情報を不正に取得することを困難にする暗号入力装置及び暗号入力方法に関する。また、利用者が暗号を入力する過程において、第三者が利用者の個人情報を不正に取得することを困難にする携帯端末に関する。

【 0 0 0 2 】

【従来の技術】

従来、利用者があるサービス対象を利用する権限を有しているか否かを認識する基本的な方法としては、サービス提供者が利用者に対して予め物理的なチケットやメンバーズカードを発行し、サービスを享受する時点でチケットやメンバー

ズカードを確認することで認証とする方法が採られてきた。

【 0 0 0 3 】

例えば、クレジットカードに代表される信用販売制度において、サービス提供者は、利用者によって提示されたカードに記録されたカード情報、すなわち本人情報によって利用者を確認し信用取引を行っている。この場合、利用者の認証は、利用者が所有するクレジットカードをカードリーダーに読ませるだけで利用者を認証できる。

【 0 0 0 4 】

また、クレジット（貸方）とは反対の意味をもつ、いわゆるデビット（借方）決済も1つの決済方法として定着しつつある。デビット決済サービスでは、利用者は、販売時点情報管理端末（以下、POSと記す。）に銀行のキャッシングカードを挿入し暗証番号と金額とを入力する。このとき、利用者の口座から即時に代金が引き落とされ精算ができる。

【 0 0 0 5 】

また、いわゆるインターネットの発達に伴って、利用者は、インターネットを介して物品を購入し、さらに決済することもできる。例えば、利用者は、クレジットカードの所定情報等をサービス提供者に送信するだけで決済することができる。

【 0 0 0 6 】

【発明が解決しようとする課題】

ところが、上述した従来の決済方法では、認証手続きの信頼性が低く、一連の認証手続きの随所において、第三者にカード情報を不正に取得されるおそれがあった。

【 0 0 0 7 】

例えば、クレジットカードの認証手続きは、このカードを所定のカードリーダーに読み込ませるだけである。利用者がある店で買い物をしたときの決済にクレジットカードを使用する場合には、利用者は、買い物をした後、決済手続のために自分のクレジットカードを店員に手渡す。このとき店員は、クレジットカードの情報を記憶できる別のカードリーダーにこのカードの情報を読み込ませることもで

きるし、また、この間にカードをすり替えることもできる。つまり、カードに記憶された個人情報等が第三者によって不正取得（スキミング）される可能性が大きかった。

【 0 0 0 8 】

特に、インターネットの場合では、利用者がサービス提供者に対してクレジットカードの所定情報等を送信するだけで決済できることが多い。従来では、通信過程で第三者によって盗聴され、クレジットカードの情報が盗まれるおそれもあった。また、インターネットの場合、サービス提供者と利用者との直接的なコンタクトが無い場合、決済のための通信課程で第三者がカード所有者本人になりすまして虚偽の決済を不正に行ったり、第三者によって決済データ等を改竄される危険性もあるため、信頼性に乏しいという問題点があった。

【 0 0 0 9 】

また、デビット決済では、キャッシングカードは、POSに挿入される。利用者は、POSの入力手段を通じて暗証番号を入力するため、例えば、POSの入力手段等に細工がされていた場合、第三者による暗証番号の不正取得が可能である。或いは、POSの入力手段の周辺に人目を隔てるような遮蔽手段等が設置されていない場合には、単にカード利用者が暗証番号を入力しているところを盗み見ることによって、第三者による暗証番号の不正取得は容易に可能となる。そして、暗証番号がスキミングされた上でカードを盗まれたり、カードをすり替えられたりすれば、カード所有者本人が気付くまで不正利用が繰り返されるおそれがあった。

【 0 0 1 0 】

以上のように上述したサービスシステムには信頼性に関する様々な技術的問題点があり、事業（ビジネス）の観点からこの問題をみると、この信頼性上の問題が利用者にとってサービス利用に対する大きな不安感をもたらしている。その結果、POSの設置等に多大な設備投資が必要なのにも関わらず利用者数が伸びずに事業の採算がとれないという問題を生んでいる。

【 0 0 1 1 】

そこで本発明は、このような従来の実情に鑑みて提案されたものであり、サー

ビス提供者が利用者を認証する過程において、第三者が利用者の個人情報に不正に取得することが困難な認証システム及び認証方法を提供することを目的とする。また、利用者が暗号を入力する過程において、第三者が利用者の個人情報に不正に取得することが困難な暗号入力装置及び暗号入力方法を提供することを目的とする。更に、利用者が暗号を入力する過程において、第三者が利用者の個人情報に不正に取得することが困難な携帯端末を提供することを目的とする。そして、さらに、利用者のサービス利用に対する大きな不安感を払拭し、利用者の拡大を促し、事業としての採算性を向上する認証システム及び認証方法、並びに暗号入力装置及び暗号入力方法、並びに携帯端末を提供することを目的とする。

【 0 0 1 2 】

【課題を解決するための手段】

本発明に係る認証システムは、携帯端末と携帯端末とは独立して設けられ携帯端末との間で通信する認証装置とから構成される認証システムにおいて、携帯端末は、携帯端末を識別するための第1の識別情報が予め記憶された第1の識別情報記憶手段と、第1の識別情報に対応付けられた第2の識別情報を入力するための操作手段と、操作手段によって入力された上記第2の識別情報を所定の暗号生成情報に基づいて暗号化する暗号化手段と、認証装置との通信を行う第1の通信手段とを備え、認証装置は、第1の識別情報と第2の識別情報とが記憶される第2の識別情報記憶手段と、暗号生成情報を発生する暗号生成情報発生手段と、携帯端末との通信を行う第2の通信手段と、暗号化手段によって暗号化された第2の識別情報を暗号生成情報に基づいて比較し認証する比較認証手段とを備える。

【 0 0 1 3 】

以上のような認証システムは、携帯端末において、操作手段により入力された第2の識別情報を第1の通信手段を介して認証装置から受信した暗号生成情報に基づいて暗号化し、暗号化された第2の識別情報を第1の通信手段を介して認証装置に送信し、該認証装置において、第2の通信手段を介して受信した暗号化された第2の識別情報と第2の識別情報記憶手段に記憶された第2の識別情報とを暗号生成情報に基づいて比較し認証することにより、上述の目的を達成する。

【 0 0 1 4 】

また、本発明に係る認証方法は、第 1 の識別情報記憶手段に予め記憶された携帯端末を識別するための第 1 の識別情報に対応付けられた第 2 の識別情報を入力する操作工程と、暗号生成情報を発生する暗号生成情報発生工程と、操作工程において入力された第 2 の識別情報を暗号生成情報発生工程において発生された暗号生成情報に基づいて暗号化する暗号化工程と、暗号化工程において暗号化された第 2 の識別情報を暗号生成情報に基づいて比較し認証する比較認証工程とを備える。

【 0 0 1 5 】

以上のような認証方法では、操作工程において入力された第 2 の識別情報が暗号化工程において暗号生成情報に基づいて暗号化され、暗号化された第 2 の識別情報と第 2 の識別情報記憶手段に記憶された第 2 の識別情報とが暗号生成情報に基づいて比較され認証されることにより、上述の目的が達成される。

【 0 0 1 6 】

さらに、本発明に係る暗号入力装置は、所定の文字群に含まれる文字の組み合わせから構成される所定数の文字列を認証用文字列とする暗号入力装置において、所定の文字群に含まれる文字を不規則に表示する表示手段と、表示手段に不規則に表示される文字のなかから認証用文字列を構成する文字を選択するための選択手段とを備える。

【 0 0 1 7 】

以上のような暗号入力装置は、表示手段に不規則に表示された所定の文字群に含まれる文字のなかから認証用文字列を構成する文字を選択手段において選択することによって、上述した目的を達成する。

【 0 0 1 8 】

さらにまた、本発明に係る暗号入力方法は、所定の文字群に含まれる文字を不規則に表示する表示工程と、表示工程において不規則に表示される文字のなかから認証用文字列を構成する文字を選択する選択工程とを備える。

【 0 0 1 9 】

以上のような暗号入力方法では、表示工程において不規則に表示される所定の文字群のなかから認証用文字列を構成する文字が選択工程において選択されるこ

とによって、上述の目的が達成される。

【 0 0 2 0 】

さらにまた、本発明に係る携帯端末は、認証装置によって認証される携帯端末において、携帯端末を識別するための第 1 の識別情報が記憶された第 1 の識別情報記憶手段と、第 1 の識別情報に対応付けられた第 2 の識別情報を入力するための操作手段と、認証装置との通信を行う通信手段と、操作手段によって入力された第 2 の識別情報を上記通信手段を介して認証装置から送られる所定の暗号生成情報に基づいて暗号化する暗号化手段とを備える。

【 0 0 2 1 】

以上のような携帯端末は、操作手段において入力された第 1 の識別情報に対応付けられた第 2 の識別情報を通信手段を介して認証装置から送られる所定の暗号生成情報に基づいて暗号化手段において暗号化することにより、上述の目的を達成する。

【 0 0 2 2 】

さらにまた、本発明に係る認証システムは、携帯端末と携帯端末とは独立して設けられ携帯端末との間で通信する認証装置とから構成される認証システムにおいて、携帯端末は、携帯端末を識別するための第 1 の識別情報が記憶された第 1 の識別情報記憶手段と、所定の文字群に含まれる文字を不規則に表示する表示手段と表示手段に不規則に表示される文字のなかから第 2 の識別情報を構成する文字を選択するための選択手段とを有し、第 1 の識別情報に対応付けられた第 2 の識別情報を入力するための操作手段と、操作手段によって入力された第 2 の識別情報を所定の暗号生成情報に基づいて暗号化する暗号化手段と、認証装置との通信を行う第 1 の通信手段とを備え、認証装置は、第 1 の識別情報と第 2 の識別情報とを記憶した第 2 の識別情報記憶手段と、暗号生成情報を発生する暗号生成情報発生手段と、携帯端末との通信を行う第 2 の通信手段と、暗号化手段によって暗号化された第 2 の識別情報を暗号生成情報に基づいて比較し認証する比較認証手段とを備える。

【 0 0 2 3 】

以上のような認証システムは、操作手段により入力された第 2 の識別情報を第

1 の通信手段を介して認証装置から受信した暗号生成情報に基づいて暗号化し、暗号化された第 2 の識別情報を第 1 の通信手段を介して認証装置に送信し、該認証装置において、第 2 の通信手段を介して受信した暗号化された第 2 の識別情報と第 2 の識別情報記憶手段に記憶された第 2 の識別情報とを暗号生成情報に基づいて比較し認証することにより、上述した目的を達成する。

【 0 0 2 4 】

【発明の実施の形態】

本発明の一構成例として示す認証システムは、携帯端末と携帯端末とは独立して設けられ携帯端末との間で通信する認証装置とから構成される認証システムである。

【 0 0 2 5 】

本発明の一構成例として示す認証システムに適用される携帯端末は、少なくとも、携帯端末を識別するためにサービスの提供者から予め付与された第 1 の識別情報が記憶された第 1 の識別情報記憶部と、第 1 の識別情報に対応付けられた第 2 の識別情報を入力するための操作部と、操作部によって入力された第 2 の識別情報を所定の暗号生成情報に基づいて暗号化する暗号化部と、認証装置との通信を行う第 1 の通信部とを備えている。また、認証装置は、少なくとも、第 1 の識別情報と第 2 の識別情報とが記憶される第 2 の識別情報記憶部と、暗号生成情報を発生する暗号生成情報発生部と、携帯端末との通信を行う第 2 の通信部と、暗号化部によって暗号化された第 2 の識別情報を暗号生成情報に基づいて比較し認証する比較認証部とを備えている。上述の携帯端末と認証装置との間では有線通信又は無線通信によって接続されることで情報の送受信が行われる。

【 0 0 2 6 】

これら携帯端末と認証装置によって構成される認証システムは、携帯端末において、操作部により入力された第 2 の識別情報を認証装置から受信した暗号生成情報に基づいて暗号化し、暗号化された第 2 の識別情報を認証装置に送信し、認証装置において、受信した暗号化された第 2 の識別情報と第 2 の識別情報記憶部に記憶された第 2 の識別情報とを暗号生成情報に基づいて比較し認証することによって、サービスの提供者が利用者を認証するまでの過程において、第三者が利

用者の個人情報を不正に取得することを困難にする認証システムである。

【 0 0 2 7 】

このような本発明に係る認証システムは、例えば、専用のネットワークを介して行われる信用販売制度（クレジットカードサービス）及び口座間即時決済（デビットカードサービス）、又はインターネットのような任意のネットワークを介して行われる電子商取引において、サービス提供者が所定のサービスを提供する利用者を認証するための認証システムとして適用することができる。この場合、携帯端末は、サービス提供者がサービス利用者に対して発行するカード形状を呈する端末であり、認証装置は、サービス提供者がサービス利用者の利用者情報を認証するためのホストコンピュータに含まれる認証装置に相当する。携帯端末としては、カード状端末のほかに P D A（Personal Digital Assistant）、携帯型電話機、携帯型 P C 等が適用できる。

【 0 0 2 8 】

本発明に係る認証システムにおいて、認証装置が携帯端末とその所有者とを認証する基本的な処理について図 1 を用いて説明する。

【 0 0 2 9 】

携帯端末の所有者は、携帯端末を使用して所定のサービスを受けようとするとき、携帯端末に第 2 の識別情報を入力する（ステップ S 1）。このときの第 2 の識別情報とは、第 1 の識別情報に対応付けされて携帯端末の所有者に与えられた、例えば暗証番号のような認証用文字列である。この認証用文字列としての暗証番号及び後述する携帯端末固有の識別情報である第 1 の識別情報は、予めサービス提供者から付与されたものである。

【 0 0 3 0 】

携帯端末は、第 1 の識別情報記憶部に記憶された第 1 の識別情報を認証装置に対して送信する（ステップ S 2）。ここで第 1 の識別情報は、認証装置が該携帯端末が管理下にあるか否かを示す情報であり、認証装置中に設けられた第 2 の識別情報記憶部に携帯端末所有者の識別用文字列と対応付けられてともに記憶されている。

【 0 0 3 1 】

続いて、認証装置は、携帯端末から第1の識別情報を取得し、該携帯端末が認証装置の管理下にあることを確認すると、携帯端末に対して、情報を暗号化するための情報（暗号鍵）、例えば、乱数を発生し送信する（ステップS3）。ここで発生された乱数は、携帯端末の第1の識別情報に対応付けられて認証装置中に暫定的に記憶される。この乱数は、携帯端末が認証用文字列を認証装置に送信する際に、認証用文字列を暗号化し秘匿するために用いられる。認証用文字列は、携帯端末の暗号化部において所定の規則に基づいて暗号化される。暗号化の規則には、既存の暗号化方法が適用できる。携帯端末は、暗号化された認証用文字列を認証装置に送信する（ステップS4）。

【0032】

認証装置は、携帯端末から暗号化された認証用文字列を受信すると、認証装置中に設けられた第2の認証情報記憶部に第1の識別情報と対応付けられて記憶されている携帯端末所有者の認証用文字列と、携帯端末から送られた暗号化された認証用文字列とを比較する。そして、携帯端末からの認証用文字列が認証装置の第2の識別情報記憶部に記憶された認証用文字列と一致した場合には、例えば、携帯端末に認証用文字列を入力した人物がその携帯端末の真の所有者であることを認証する（ステップS5）。

【0033】

また、第2の認証情報記憶部に第1の識別情報と対応付けられて記憶されている携帯端末所有者の認証用文字列と、暗号化された認証用文字列との比較は、暗号化された認証用文字列を先ず認証装置中に暫定的に記憶しておいた暗号化用の乱数を用いて復号した後、その結果を認証装置に記憶された認証用文字列と比較することによって行われる。或いは、逆に、認証装置に記憶された認証用文字列を乱数によって携帯端末において用いられた暗号化規則と同一の規則により暗号化し、その結果を携帯端末からの暗号化された認証用文字列と比較してもよい。このように、携帯端末の所有者が所定のサービスを受けようとする毎に乱数を発生させ、この乱数に基づいて暗号化することにより、携帯端末から送信される暗号化された認証用文字列は、常に異なった符号で表現されるために、秘匿性がより高まる。

【 0 0 3 4 】

携帯端末は、認証装置によって認証されると記憶された認証用文字列を消去する。認証装置は、認証された携帯端末に対して、所定の処理を実行する（ステップ S 6）。

【 0 0 3 5 】

上述の処理において、携帯端末と認証装置とが接続されるタイミングは、限定されない。すなわち、携帯端末は、まず認証用文字列が入力された状態で認証装置に接続されてもよいし、第一段階としてまず認証装置に接続されて乱数を取得した後、一旦接続が解除され認証用文字列が入力された後、再度接続がなされてもよい。

【 0 0 3 6 】

本発明に係る認証システムでは、以上の処理によって、認証装置が携帯端末を認証している。本発明に係る認証システムでは、携帯端末は、所有者によって、例えば暗証番号のような認証用文字列が入力されなければ、単体で認証装置に認証されることはできないようになっているため、第三者が携帯端末だけを用いて不正行為を働くことができないようになっている。しかし、所有者が携帯端末に認証用文字列を入力する際には高い秘匿性が要求されることには変わらない。

【 0 0 3 7 】

そのため、本発明に係る認証システムでは、暗証番号としての認証用文字列の入力部は、所定の文字群に含まれる文字を不規則に表示する表示部と、表示部に不規則に表示される文字のなかから認証用文字列を構成する文字を選択するための選択部を備える構成とされている。例えば、表示部では、0 から 9 で表される 1 0 個の数字該表示部の任意の位置に 0 から 9 で表される 1 0 個の数字を不規則に表示される。更に、携帯端末は、該携帯端末内に認証装置との間の認証に使用される認証用文字列が保持されないために秘匿性が高められている。

【 0 0 3 8 】

このように本発明に係る認証システムは、認証装置が該携帯端末が認証装置に管理されるか否かを認証する際に、認証装置（サービスの提供者）が携帯端末（利用者）を認証するまでの過程において、第三者がカード情報や端末情報を不正

取得することを困難にすることを実現した認証システムである。

【 0 0 3 9 】

特に、本発明に係る認証システムでは、利用者が、例えばクレジット（貸方）カードを用いた信用取引制度、銀行のキャッシュカードを用いたデビット（借方）決済サービスを利用する際に、サービスの提供者或いは利用者に対して物品を販売した販売者が利用者によって提示されたカードに記録された利用者本人の情報を認証し、その認証に基づいて決済する場合を想定している。そのため本実施の形態では、携帯端末は、サービスの提供者から利用者に対して予め発行される「カード」として示す。また、サービスは、主に物品購入の際の「決済」を示す。

【 0 0 4 0 】

この携帯端末としてのカードは、従来のこのようなサービスにおける利用者の個人認証に用いられるカードとは異なり、認証用文字列（暗証番号）を入力する入力部と、所定の暗号生成情報に基づいてホストコンピュータに対する認証用情報を生成する情報暗号化部とを備えている点が特徴である。情報暗号化部は、サービスの提供者側の認証装置から送信される所定の暗号生成情報（暗号鍵）、例えば、乱数とカード自身に予め記憶されたカードの認証情報としてのカードIDとを混合して符号化し、ホストコンピュータに対する認証用情報を生成する。また、この携帯端末としてのカードの入力部は、利用者が暗証番号を入力する際、十分な秘匿性が確保された入力部とされている。

【 0 0 4 1 】

つまり、この携帯端末としてのカードは、カード所有者によって暗証番号が入力されることが必要であって、カード単体では認証を目的としたカード本来の機能を果たさず、例えば、従来のカードのようにカードリーダーで読み取るといった単純な動作のみでは認証装置によって認証されないようになっている。

【 0 0 4 2 】

以下、本発明に係る認証システム1について、図面を参照して詳細に説明する。図2に示すように、認証システム1は、カード10と認証装置としてのホストコンピュータ20とが接続線30で接続されて構成される認証システムである。

ホストコンピュータ 20 は、カード 10 と接続された際、カード 10 が該ホストコンピュータ 20 が管理するカード 10 であるかを判断し、更にカードに記憶されたカード所有者の個人情報等を入手してカード 10 とその所有者を認証するものである。

【0043】

ここで、接続線 30 は、ホストコンピュータ 30 に接続するための専用回線、または、複数のネットワーク同士を接続して大規模なネットワークとして構成される所謂インターネットである。また、接続線 30 を介してホストコンピュータ 20 とカード 10 とを接続する形態には種々の形態が考えられる。例えば、ホストコンピュータ 20 は、カード 10 を接続するための接続端末を備え、該接続端末との間で接続線を介して接続される場合も考えられる。この場合は、接続端末とホストコンピュータ 20 との間が有線通信又は無線通信で接続される。カードと接続端末との間の接続は、磁気による読み取りや接続端子による接触接続でもよいし、非接触接続であってもよい。

【0044】

カード 10 は、該カードの識別情報であって上述の第 1 の識別情報に相当するカード ID を記憶するための ID 用メモリ 11 と、カード所有者によって認証用文字列としての暗証番号の入力等が行われる入力部 12 と、ホストコンピュータ 20 と接続線 30 を介して接続されるカード側インターフェイス 13 とを備えている。カード ID は、該カードを特定するための情報であってサービス提供者から予め付与されたものである。このカード ID は、所有者個人を特定する直接的な情報を示すものではない。入力部 12 は、認証用文字列としての暗証番号が入力されるため、第三者によってカード所有者の暗証番号を不正に取得されないような構成とされている。入力部 12 についての詳細は、後述する。

【0045】

カード 10 は、更に、情報暗号化部 14 と一時記憶部 15 と表示部 16 とを備えている。情報暗号化部 14 は、ホストコンピュータ 20 から送られ、送信される毎に固有の値を有する上述した所定の暗号生成情報に相当する乱数と該カードの識別番号としてのカード ID とを混合して符号化しホストコンピュータ 30 に

対する認証用情報を生成している。また、一時記憶部 1 5 には、入力部より入力された暗証番号が一時的に記憶されている。一時記憶部 1 5 に記憶された暗証番号は、認証が終了する毎、または所定時間毎に消去される。表示部 1 6 としては、例えば、液晶表示装置が用いられる。表示部 1 6 は、入力部 1 2 で入力の際に必要なとなる情報等を表示する。ここで、情報暗号化部 1 4 における暗号化方法としては、種々の暗号化方法が適用可能である。

【 0 0 4 6 】

カード 1 0 において上述した各部は、CPU (Central Processing Unit) と該 CPU のワークエリアとしての RAM (Random Access Memory) と各種処理を行うためのプログラム等を記憶する ROM (Read Only Memory) とを有するカード制御部 1 7 によって統括制御されている。また、カード制御部 1 7 は、カード ID 及び認証用情報をホストコンピュータ 2 0 へ送信する制御を行うほか、認証用情報として送信された認証用文字列がホストコンピュータ 2 0 に認証されると一時記憶部 1 5 に記憶された暗証番号を消去する。カード制御部 1 7 は、所定時間毎に一時記憶部 1 5 の記憶内容を消去することもできる。

【 0 0 4 7 】

このように、カード 1 0 は、暗証番号をホストコンピュータ 2 0 との通信毎に異なる暗号鍵によって符号化するうえ、入力された暗証番号が該カード内に保持されないため、万が一第三者によって盗難されることがあっても、カード単体ではホストコンピュータ 2 0 に認証されない。

【 0 0 4 8 】

ホストコンピュータ 2 0 は、カード 1 0 と接続線 3 0 を介して接続されるホスト側インターフェイス 2 1 と、乱数を生成する乱数生成部 2 2 と、カード 1 0 のカード ID とカード ID に対して発行した認証用文字列とを対応付けて保持するカード ID / 認証用文字列記憶部 2 3 と、認証用情報を復号してカードの認証情報を抽出する情報復号部 2 4 と、カード 1 0 における情報暗号化部 1 4 によって乱数とカード ID とを混合して符号化された認証用情報を発生した乱数に基づいて比較し認証する復号認証用文字列比較認証部 2 5 とを備えている。また、これらの各部は、CPU と該 CPU のワークエリアとしての RAM と各種処理を行う

ためのプログラム等を記憶するROMとを有するホスト制御部26によって統括制御されている。また、カードID／認証用文字列記憶部23には、乱数生成部22において生成された乱数を発生したカードIDに対応付けて記憶される。

【0049】

ここで、乱数生成部22は、所定のタイミングで所定の関数によって暗号鍵を生成するものであればよい。例えば、全方位測位システム（GPS）やクロック等から得られた情報に基づいて、所定の関数によってその都度得られた固有の値を暗号鍵とする暗号鍵生成部を用いることもできる。また、ホスト制御部26は、カードから送られたカードIDとともにそのカードに対して発行した乱数を対応付けしてカードID／認証用文字列記憶部23に一時的に保持する。更に、ホスト制御部26は、情報復号部24を制御して認証用情報からカードの識別情報を抽出し、復号認証用文字列比較認証部25において比較し認証された場合、カード所有者に対して所定のサービスを提供する。

【0050】

上述した認証システム1では、カードID／認証用文字列記憶部23にカードIDと対応付けられて記憶されている携帯端末所有者の認証用文字列と、情報暗号化部14によって暗号化された認証用文字列（認証用情報）との比較は、暗号化された認証用文字列（認証用情報）を、先ずホストコンピュータ20に暫定的に記憶しておいた乱数を用いて復号した後、その結果をカードID／認証用文字列記憶部23に記憶された認証用文字列と比較することによって行われるが、逆に、カードID／認証用文字列記憶部23に記憶された認証用文字列をカード10において行われる暗号化と同一の規則により暗号化し、その結果をカード10からの暗号化された認証用文字列（認証用情報）と比較してもよい。

【0051】

すなわち、認証システム1におけるホストコンピュータ20は、図3に示すように、情報復号部24の代わりに情報暗号化部14と同一の規則により暗号化するホスト側情報暗号化部27を備え、復号認証用文字列比較認証部25の代わりに暗号認証用情報文字列比較認証部28を備える。この場合、カードID／認証用文字列記憶部23に記憶された認証用文字列をカード10において行われる暗

号化と同一の規則により暗号化することによって、認証用情報を復号することなく比較し認証できる。

【 0 0 5 2 】

上述したように、カード 1 0 は、入力部 1 2 において所有者からの暗証番号の入力がなされる。そのため入力部 1 2 は、所有者が暗証番号を入力する際、第三者に対して十分な秘匿性が確保されていなければならない。以下、高い秘匿性をもって暗証番号の入力を可能とする入力部 1 2 の具体例を、図 4 乃至図 6 に示す。従来、ホストコンピュータ或いはホストコンピュータの接続端末等は、固定された入力部から暗証番号を入力する方法が採られていたが、この場合、入力時に暗証番号を第三者から秘匿することが困難であった。カード 1 0 は、該カードに暗証番号が入力できるためカード所有者が暗証番号を入力する際、任意の場所での入力が可能である。つまり、カード所有者は、暗証番号を入力する場면을第三者の目から保護できる。したがって、入力部 1 2 は、暗証番号入力時の機密性が確保される構成となっている。

【 0 0 5 3 】

図 4 には第 1 の実施例として示す入力部 1 2 を備えたカード 1 0 の外観の概略が示されている。図 4 に示すカード 1 0 において、表示部 1 6 は、該表示部の任意の位置に、その都度不規則に 1 0 個の数字の各々を表示することを特徴としている。また、入力部 1 2 は、例えば、接触された位置を検出し、その位置情報を入力に反映するような接触入力機能を備えた入力部であって、表示部 1 6 の対応位置に重ねて設けられている。

【 0 0 5 4 】

図 4 では、表示部 1 6 に左上から右下にかけて 7, 8, 4, 3, 1, 5, 0, 6, 2, C, 9, E が表示されている場合が示されている。次回入力の際には、それぞれの数字は、表示部 1 6 の別の位置に表示される。図 4 に示す「C」は、選択ボタンを示し、「E」は、消去ボタンを示している。暗証番号を入力する際、カードの所有者は、表示部 1 6 に不規則に表示される数字のうち所望の数字に触れて暗証番号としての文字列を入力し、入力が終わった時点で「C」ボタンを押す。「E」ボタンは、入力した数字を訂正する場合、又は暗証番号として入力

した文字列を消去する場合に用いられる。

【 0 0 5 5 】

表示部の所定位置に決められた数字が表示される場合、カード所有者が暗証番号を入力する都度同じ箇所が押される。この場合、回数を重ねて使用するうちに、該入力部 1 2 の摩耗・汚れによって暗証番号として使用している数字が第三者に知られてしまうおそれがある。また、入力時に数字を指す指の動き等によっても暗証番号が明らかになるおそれがあるが、図 4 に示す入力部を備えるカード 1 0 の場合、少なくとも該入力部 1 2 の摩耗・汚れ、或いは入力時の動作等によって暗証番号として使用する数字が第三者に知られることは困難である。

【 0 0 5 6 】

次に、入力部 1 2 の第 2 の実施例について図 5 を用いて説明する。図 5 に示すカード 1 0 において、表示部 1 6 は、予めカード表面に記された上記 0 から 9 の数字若しくはこの数字の近傍を発光させることで各々の数字を指し示すことを特徴としている。この場合、表示部 1 6 は、例えば L E D (Light Emitting Diode) のような発光手段であって、所定の数字を示すように発光する。表示部 1 6 は、0 から 9 へ、又は 9 から 0 へ順番に順次発光されてもよいし、不規則な順序で発光されてもよい。また、発光期間も同様に一定でも不規則でもよい。

【 0 0 5 7 】

この場合、入力部 1 2 は、選択ボタン「S」と消去ボタン「E」とを備えているが、選択の際に用いられる入力部 1 2 のボタンは、「S」1 つである。各表示部 1 6 は、順番に、或いは不規則に発光するため、カードの所有者は、所望とする数字が指し示されたときに選択ボタンを押せばよい。この場合、暗証番号としての文字列の選択に際して、常に同じ箇所が押されるため、ボタンの摩耗・汚れ、或いは入力時の動作等によって暗証番号として使用する数字が第三者に知られることは困難である。

【 0 0 5 8 】

続いて、入力部 1 2 の第 3 の実施例について図 6 を用いて説明する。図 6 に示すカード 1 0 において、表示部 1 6 は、1 0 個の数字のうち 1 つの数字を表示することを特徴としている。表示部 1 6 は、1 0 個の数字を順番に表示してもよい

し不規則に表示してもよい。利用者は、所望の数字が表示されたときに入力部 12 の選択ボタン「S」を押すことによって、所望の数字を選択することができる。

【0059】

この場合も、入力部 12 は、数字の選択に際して、常に 1 つのボタンが押されるのみであるため、少なくとも摩耗・汚れ、或いは入力時の動作等によって第三者に暗証番号として使用する数字が知られることは困難である。

【0060】

上述した 3 つの実施例は、表示部 16 の視野角を狭く設定することによって、暗証番号を入力する際の秘匿性を更に高めることが可能である。

【0061】

なお、本発明は、携帯端末としてのカード自身に暗証番号の入力機能をもたせた点に特徴を有するものであるため、カード 10 とホストコンピュータ 20 との間の信号の送受信における暗号化方法は、特に限定されず、現在汎用の暗号化原理、公開鍵暗号方式等の暗号化原理が適用可能である。暗号化方法の一例としては、認証装置としてのホストコンピュータ 20 からカード 10 に対して送信される乱数とカード 10 の暗証番号とを所定の規則のもとで演算して得られた値をカード 10 のホストコンピュータ 20 に対する暗号鍵とするものが考えられる。

【0062】

ここでは、具体的に、ホストコンピュータ 20 が発生する乱数が 20 桁であり、カード 10 の暗証番号が 4 桁であり、更にカード 10 の情報暗号化部 14 において暗証番号と乱数とから 4 桁の値を認証用情報として生成する場合を説明する。

【0063】

ホストコンピュータ 20 からカード 10 に対して送信された 20 桁の数字を 5 桁の数字からなる 4 組の数字に並び換える並べ方は、 $20!$ 通り、すなわち約 2.4×10^{18} 通りある。また、このとき 20 桁の数字を 5 桁の 4 つの数字に並び換える規則としては、例えば、最初の 5 桁の数字の 1 番目は 20 桁の乱数の 19 桁目の数字とし、2 番目は 3 桁目の数字とし、3 番目は、17 桁目の数字とし

、4番目は5桁目の数字とし、5番目は15桁目の数字として5桁の数字を決める方法等が考えられる。

【0064】

次に5桁の数字からなる4組の数字の各々に4桁の数字からなる暗証番号の1桁ずつを挿入して6桁の数字を作る。6カ所の挿入可能な位置に対して、どの位置に挿入するかを決める。このときの挿入の仕方は、 $(10 \times 6)^4$ 通り、つまり約 1.3×10^7 通りが考えれる。

【0065】

ここでは更に、20桁からなる乱数から5桁からなる数字を4つ決めておき前段階で作成された6桁の数字と掛け合わせる。掛け合わせる際の掛け合わせ方は、 $(10^5)^4$ 通り、すなわち 10^{20} 通りが考えられる。この掛け合わせによって、11桁又は12桁の数字が4組得られる。

【0066】

次に、この11桁又は12桁の数字の下10桁のなかから任意の1桁を抽出する。4組の数字についてこの操作を行って抽出された4つ数字を組み合わせ、この数字を4桁の認証用情報とする。この選び方は、 10^4 通りあることになる。

【0067】

したがって、上述のような極めて単純な場合であっても、20桁の乱数と4桁の暗証番号の混合によって、約 3.1×10^{49} 通りの認証用情報が得られることになる。尚かつ、最終的に認証用情報とする値は、4桁であって比較的小さい値であるので、たとえ上述した暗号化のための演算が分かったとしても、数〜数十回のスキミングで各数値を逆算することは困難であるといえる。

【0068】

このように認証システム1におけるカード10の入力部12によれば、利用者が認証用文字列としての暗証番号を入力する際の秘匿性が向上する。

【0069】

続いて、上述した認証システム1を適用して行われる決済の具体例を図7乃至図8を用いて説明する。カード所有者が店頭にて購入した商品に対してカードを使用して決済する場合について、図7を用いて示す。カード所有者50は、販売

店 5 1 において商品を選択する（行程 7 1）。購入する商品が決まると、販売店 5 1 では、カード所有者が会計する際にパーソナルコンピュータ（以下、P C と記す。）等の専用のネットワーク端末 5 2 をカード発行会社 5 3 に接続し（行程 7 2）、商品の内容と金額情報とを送信する（行程 7 3）。カード所有者 5 0 は、購入する商品の商品情報（商品の内容と金額情報）を確認し（行程 7 4）、カード 5 4 に暗証番号を入力する（行程 7 5）。暗証番号が入力されたカード 5 4 は、専用のネットワーク端末 5 2 に接続される（行程 7 6）。このとき、上述した決済プロセスが実行される。決済が完了するとカード発行会社 5 3 から決済完了レシートが送信される（行程 7 7）。

【 0 0 7 0 】

この場合、カード所有者がカードに対して暗証番号を入力する際、第三者の目の届かないところで入力が可能である。また、決済の過程でカード 5 4 が販売店員の手に渡ることがあるが、このとき暗証番号を入力したカードを見られたとしても、入力した形跡から第三者が暗証番号を不正取得することは困難である。また、仮にカードがすり替えられたとしても、暗号化に使用される暗号化情報が通信毎に固有であるため、そのとき暗号化されて生成された認証用情報は、その通信以外では無効になる。したがって、第三者が不正に個人情報を取得することは困難である。

【 0 0 7 1 】

次に、カード所有者が高級飲食店等においてカードを使用して決済する場合について、図 8 を用いて示す。ここでは、高級飲食店での決済として説明するが図 8 に示す決済の形態は、一般に、カード 5 4 が、一旦、給仕等の第三者の手に渡る場合を想定している。カード所有者 5 0 は、給仕の提示する料金明細書等を確認しチップ等の金額を記入する（行程 8 1）。また、カード 5 4 に対して暗証番号を入力（行程 8 2）して、料金明細書とともにカード 5 4 を給仕に渡す（行程 8 3）。給仕 5 5 は、カード所有者からカード 5 4 を受け取ると、販売店（飲食店） 5 1 に設置された P C 等の専用のネットワーク端末 5 2 をカード発行会社 5 3 に接続し、商品情報（商品の内容と金額情報）とを送信する（行程 8 4）。続いて、カード所有者 5 0 から預かったカード 5 4 をネットワーク端末 5 2 に接続

する（行程 85）。ここで、上述した決済プロセスが実行される（行程 86）。決済が完了するとカード発行会社 53 から決済完了レシートが送信される（行程 87）。給仕 55 は、決済完了レシートとともに、カード 54 をカード所有者 50 のもとへ返却する（行程 88）。

【0072】

この場合もまた、カード所有者がカードに対して暗証番号を入力する際、第三者の目の届かないところで入力が可能である。また、決済の過程でカード 54 が第三者の手に渡ることがあるが、このとき暗証番号を入力したカードを見られたとしても、入力した形跡から第三者が暗証番号を不正取得することは困難である。また、仮にカードがすり替えられたとしても、暗号化に使用される暗号化情報が通信毎に固有であるため、そのとき暗号化されて生成された認証用情報は、その通信以外では無効になる。したがって、第三者が不正に個人情報を取得することは困難である。

【0073】

次に、カード所有者がカードを使用して、いわゆるインターネットを介して決済する場合について、図 9 を用いて示す。ここでは、インターネットに接続される PC 等の端末がカード 54 を装着してカードの情報を読み出せる読出装置を備えているものとする。ここでは、主としてカード所有者 50 が自宅の PC 等を使用する場合を想定しているが、店頭等に設置されたインターネットに接続された PC 等を使用する場合も含まれる。カード所有者 50 は、インターネットに接続された PC 等のネットワーク端末 56 を介して、販売店 51 において販売されている商品をインターネット上から選択する（行程 91）。続いて、カード所有者 50 は、サービスを受けているカード発行会社を選択する（行程 92）。続いて、カード所有者 50 は、商品情報（商品の内容と金額情報）を送信する（行程 93）。商品情報は、販売店 51 を介してもカード発行会社 53 に送信される。カード所有者 50 は、商品情報を確認する（行程 94）。カード所有者 50 は、カード 54 に対して暗証番号を入力する（行程 95）。ここで、上述の決済プロセスが実行される（行程 96）。カード発行会社 53 からは、決済完了を示す情報が送信される（行程 97）。

【 0 0 7 4 】

この場合、カード所有者がカードに対して暗証番号を入力する際、第三者の目の届かないところで入力が可能である。特に、P C が店頭等に設置され不特定多数の利用者が利用するものであり、P C 内部に何らかの形で個人情報が残されたり、インターネットによる情報の送受信の過程で個人情報が盗聴されたりする不都合があったとしても、暗号化に使用される暗号化情報が通信毎に固有であるため、そのとき暗号化されて生成された認証用情報は、その通信以外では無効になる。したがって、第三者が不正に個人情報を取得することは困難である。

【 0 0 7 5 】

上述したように、本発明の一構成例として示す認証システム 1 を専用のネットワークを介して行われる信用販売制度及び口座間即時決済等に適用した際、利用者が認証用文字列としての暗証番号を入力する際の秘匿性が向上する。また、サービス利用者のカード利用における信頼性に対する不安が払拭されることにより、いわゆるクレジットカードを利用する信用販売制度、キャッシュカードを利用する口座間即時決済、通信端末を利用してインターネット等の任意のネットワークを介して行われる電子商取引等の利用者が増加するとともに市場が拡大され、事業としての採算性が向上される。

【 0 0 7 6 】

また、本発明は上述した実施の形態のみに限定されるものではなく、本発明の要旨を逸脱しない範囲において種々の変更が可能であることは勿論である。例えば、本発明の一構成例として示した認証システム 1 では、携帯端末が符号化回路を備えたカードとして説明したが、携帯端末としては、カードのほかに P D A (Personal Digital Assistant)、携帯型電話機、携帯型 P C 等であってもよい。携帯型電話機、或いは P D A、P C に格納される個人情報等は、クレジットカード、デビットカードにおけるカード情報と同様に第三者に漏洩しては困る情報である。携帯型電話機を使って上述したような決済が行われる場面は、容易に想定される。例えば、使用者がある店舗で買い物をした後、自らが所有する携帯型電話機に記憶される個人情報等を用いて決済を行う場合等である。この場合もまた、図 1 に示す処理によって認証装置との間で認証が行われる。

【 0 0 7 7 】

したがって、カード以外の携帯端末を用いた認証システムであっても、サービスの提供者が利用者を認証するまでの過程において、第三者が端末情報や個人情報などを不正に取得することを困難にすることができる。

【 0 0 7 8 】

【発明の効果】

以上詳細に説明したように、本発明に係る認証システムは、携帯端末と携帯端末とは独立して設けられ携帯端末との間で通信する認証装置とから構成される認証システムにおいて、携帯端末は、携帯端末を識別するための第1の識別情報が予め記憶された第1の識別情報記憶手段と、第1の識別情報に対応付けられた第2の識別情報を入力するための操作手段と、操作手段によって入力された上記第2の識別情報を所定の暗号生成情報に基づいて暗号化する暗号化手段と、認証装置との通信を行う第1の通信手段とを備え、認証装置は、第1の識別情報と第2の識別情報とが記憶される第2の識別情報記憶手段と、暗号生成情報を発生する暗号生成情報発生手段と、携帯端末との通信を行う第2の通信手段と、暗号化手段によって暗号化された第2の識別情報を暗号生成情報に基づいて比較し認証する比較認証手段とを備える。

【 0 0 7 9 】

以上のような認証システムは、携帯端末において、操作手段により入力された第2の識別情報を第1の通信手段を介して認証装置から受信した暗号生成情報に基づいて暗号化し、暗号化された第2の識別情報を第1の通信手段を介して認証装置に送信し、該認証装置において、第2の通信手段を介して受信した暗号化された第2の識別情報と第2の識別情報記憶手段に記憶された第2の識別情報とを暗号生成情報に基づいて比較し認証する。

【 0 0 8 0 】

したがって、本発明に係る認証システムによれば、サービスの提供者が利用者を認証するまでの過程において、第三者が利用者の個人情報を不正に取得することが困難になる。

【 0 0 8 1 】

特に、本発明に係る認証システムを専用のネットワークを介して行われる信用販売制度及び口座間即時決済、又はインターネット等の任意のネットワークを介して行われる電子商取引等に適用した際、利用者が認証用文字列としての暗証番号を入力する際の秘匿性が向上する。

【 0 0 8 2 】

さらに、本発明に係る認証システムによれば、サービス利用者のカード利用における信頼性に対する不安が払拭されることにより、いわゆるクレジットカードを利用する信用販売制度、キャッシュカードを利用する口座間即時決済、通信端末を利用してインターネット等の任意のネットワークを介して行われる電子商取引等の利用者が増加し、事業としての採算性が向上する。

【 0 0 8 3 】

また、本発明に係る認証方法は、第 1 の識別情報記憶手段に予め記憶された携帯端末を識別するための第 1 の識別情報に対応付けられた第 2 の識別情報を入力する操作工程と、暗号生成情報を発生する暗号生成情報発生工程と、操作工程において入力された第 2 の識別情報を暗号生成情報発生工程において発生された暗号生成情報に基づいて暗号化する暗号化工程と、暗号化工程において暗号化された第 2 の識別情報を暗号生成情報に基づいて比較し認証する比較認証工程とを備える。

【 0 0 8 4 】

以上のような認証方法では、操作工程において入力された第 2 の識別情報が暗号化工程において暗号生成情報に基づいて暗号化され、暗号化された第 2 の識別情報と第 2 の識別情報記憶手段に記憶された第 2 の識別情報とが暗号生成情報に基づいて比較され認証される。

【 0 0 8 5 】

したがって、本発明に係る認証方法によれば、サービスの提供者が利用者を認証するまでの過程において、第三者が利用者の個人情報をも不正に取得することが困難になる。

【 0 0 8 6 】

特に、本発明に係る認証方法を専用のネットワークを介して行われる信用販売

制度及び口座間即時決済、又は任意のネットワークを介して行われる電子商取引等に適用した際、利用者が認証用文字列としての暗証番号を入力する際の秘匿性が向上する。

【 0 0 8 7 】

さらに、本発明に係る認証方法によれば、サービス利用者のカード利用における信頼性に対する不安が払拭されることにより、いわゆるクレジットカードを利用する信用販売制度、キャッシュカードを利用する口座間即時決済、通信端末を利用してインターネット等の任意のネットワークを介して行われる電子商取引等の利用者が増加し、事業としての採算性が向上する。

【 0 0 8 8 】

また、本発明に係る暗号入力装置は、所定の文字群に含まれる文字の組み合わせから構成される所定数の文字列を認証用文字列とする暗号入力装置において、所定の文字群に含まれる文字を不規則に表示する表示手段と、表示手段に不規則に表示される文字のなかから認証用文字列を構成する文字を選択するための選択手段とを備える。

【 0 0 8 9 】

以上のような暗号入力装置は、表示手段に不規則に表示された所定の文字群に含まれる文字のなかから認証用文字列を構成する文字を選択手段において選択する。

【 0 0 9 0 】

したがって、本発明に係る暗号入力装置によれば、利用者が暗号を入力する過程において、第三者が利用者の個人情報をも不正に取得することが困難になる。

【 0 0 9 1 】

特に、本発明に係る暗号入力装置を専用のネットワークを介して行われる信用販売制度及び口座間即時決済、又は任意のネットワークを介して行われる電子商取引等に使用される携帯端末、特に、カードの入力部に適用した際、利用者が認証用文字列としての暗証番号を入力する際の秘匿性が向上する。

【 0 0 9 2 】

さらに、本発明に係る暗号入力装置によれば、サービス利用者のカード利用における信頼性に対する不安が払拭されることにより、いわゆるクレジットカードを利用する信用販売制度、キャッシュカードを利用する口座間即時決済、通信端末を利用してインターネット等の任意のネットワークを介して行われる電子商取引等の利用者が増加し、事業としての採算性が向上する。

【 0 0 9 3 】

本発明に係る暗号入力方法は、所定の文字群に含まれる文字を不規則に表示する表示工程と、表示工程において不規則に表示される文字のなかから認証用文字列を構成する文字を選択する選択工程とを備える。

【 0 0 9 4 】

以上のような暗号入力方法では、表示工程において不規則に表示される所定の文字群のなかから認証用文字列を構成する文字が選択工程において選択される。

【 0 0 9 5 】

したがって、本発明に係る暗号入力方法によれば、利用者が暗号を入力する過程において、第三者が利用者の個人情報を不正に取得することが困難になる。

【 0 0 9 6 】

特に、本発明に係る暗号入力方法を専用のネットワークを介して行われる信用販売制度及び口座間即時決済、又は任意のネットワークを介して行われる電子商取引等に使用される携帯端末、特に、カード入力部での入力方法として適用した際、利用者が認証用文字列としての暗証番号を入力する際の秘匿性が向上する。

【 0 0 9 7 】

さらに、本発明に係る暗号入力方法によれば、サービス利用者のカード利用における信頼性に対する不安が払拭されることにより、いわゆるクレジットカードを利用する信用販売制度、キャッシュカードを利用する口座間即時決済、通信端末を利用してインターネット等の任意のネットワークを介して行われる電子商取引等の利用者が増加し、事業としての採算性が向上する。

【 0 0 9 8 】

本発明に係る携帯端末は、認証装置によって認証される携帯端末において、携帯端末を識別するための第 1 の識別情報が予め記憶された第 1 の識別情報記憶手

段と、第 1 の識別情報に対応付けられた第 2 の識別情報を入力するための操作手段と、認証装置との通信を行う通信手段と、操作手段によって入力された第 2 の識別情報を上記通信手段を介して認証装置から送られる所定の暗号生成情報に基づいて暗号化する暗号化手段とを備える。

【 0 0 9 9 】

以上のような携帯端末は、操作手段において入力された第 1 の識別情報に対応付けられた第 2 の識別情報を通信手段を介して認証装置から送られる所定の暗号生成情報に基づいて暗号化手段において暗号化する。

【 0 1 0 0 】

したがって、本発明に係る携帯端末によれば、利用者が暗号を入力する過程において、第三者が利用者の個人情報を不正に取得することが困難になる。

【 0 1 0 1 】

特に、本発明に係る携帯端末を専用のネットワークを介して行われる信用販売制度及び口座間即時決済、又は任意のネットワークを介して行われる電子商取引等に使用される携帯端末に適用した際、利用者が認証用文字列としての暗証番号を入力する際の秘匿性が向上する。

【 0 1 0 2 】

さらに、本発明に係る携帯端末によれば、サービス利用者のカード利用における信頼性に対する不安が払拭されることにより、いわゆるクレジットカードを利用する信用販売制度、キャッシュカードを利用する口座間即時決済、通信端末を利用してインターネット等の任意のネットワークを介して行われる電子商取引等の利用者が増加し、事業としての採算性が向上する。

【 0 1 0 3 】

本発明に係る認証システムは、携帯端末と携帯端末とは独立して設けられ携帯端末との間で通信する認証装置とから構成される認証システムにおいて、携帯端末は、携帯端末を識別するための第 1 の識別情報が記憶された第 1 の識別情報記憶手段と、所定の文字群に含まれる文字を不規則に表示する表示手段と表示手段に不規則に表示される文字のなかから第 2 の識別情報を構成する文字を選択するための選択手段とを有し、第 1 の識別情報に対応付けられた第 2 の識別情報を入

力するための操作手段と、操作手段によって入力された第 2 の識別情報を所定の暗号生成情報に基づいて暗号化する暗号化手段と、認証装置との通信を行う第 1 の通信手段とを備え、認証装置は、第 1 の識別情報と第 2 の識別情報とを記憶した第 2 の識別情報記憶手段と、暗号生成情報を発生する暗号生成情報発生手段と、携帯端末との通信を行う第 2 の通信手段と、暗号化手段によって暗号化された第 2 の識別情報を暗号生成情報に基づいて比較し認証する比較認証手段とを備える。

【0104】

以上のような認証システムは、操作手段により入力された第 2 の識別情報を第 1 の通信手段を介して認証装置から受信した暗号生成情報に基づいて暗号化し、暗号化された第 2 の識別情報を第 1 の通信手段を介して認証装置に送信し、該認証装置において、第 2 の通信手段を介して受信した暗号化された第 2 の識別情報と第 2 の識別情報記憶手段に記憶された第 2 の識別情報とを暗号生成情報に基づいて比較し認証する。

【0105】

したがって、本発明に係る認証システムによれば、サービスの提供者が利用者を認証するまでの過程において、第三者が利用者の個人情報を不正に取得することが困難になる。

【0106】

特に、本発明に係る認証システムを専用のネットワークを介して行われる信用販売制度及び口座間即時決済、又は任意のネットワークを介して行われる電子商取引等に適用した際、利用者が認証用文字列としての暗証番号を入力する際の秘匿性が向上する。

【0107】

さらに、本発明に係る認証システムによれば、サービス利用者のカード利用における信頼性に対する不安が払拭されることにより、いわゆるクレジットカードを利用する信用販売制度、キャッシュカードを利用する口座間即時決済、通信端末を利用してインターネット等の任意のネットワークを介して行われる電子商取引等の利用者が増加し、事業としての採算性が向上する。

【図面の簡単な説明】

【図 1】

本発明の一構成例として示す認証システムにおいて、認証装置が携帯端末を認証する処理を説明するフローチャートである。

【図 2】

本発明の一構成例として示す認証システムの構成を説明する構成図である。

【図 3】

本発明の一構成例として示す認証システムの別の構成を説明する構成図である。

【図 4】

本発明の一構成例として示す認証システムにおける携帯端末としてのカードの外観を示す外観図である。

【図 5】

本発明の一構成例として示す認証システムにおける携帯端末としてのカードの外観を示す外観図である。

【図 6】

本発明の一構成例として示す認証システムにおける携帯端末としてのカードの外観を示す外観図である。

【図 7】

カード所有者が店頭にて購入した商品に対してカードを使用して決済する場合を説明する模式図である。

【図 8】

カード所有者が高級飲食店等においてカードを使用して決済する場合を説明する模式図である。

【図 9】

カード所有者が P C 等のネットワーク端末を介して、インターネット上で決済する場合を説明する模式図である。

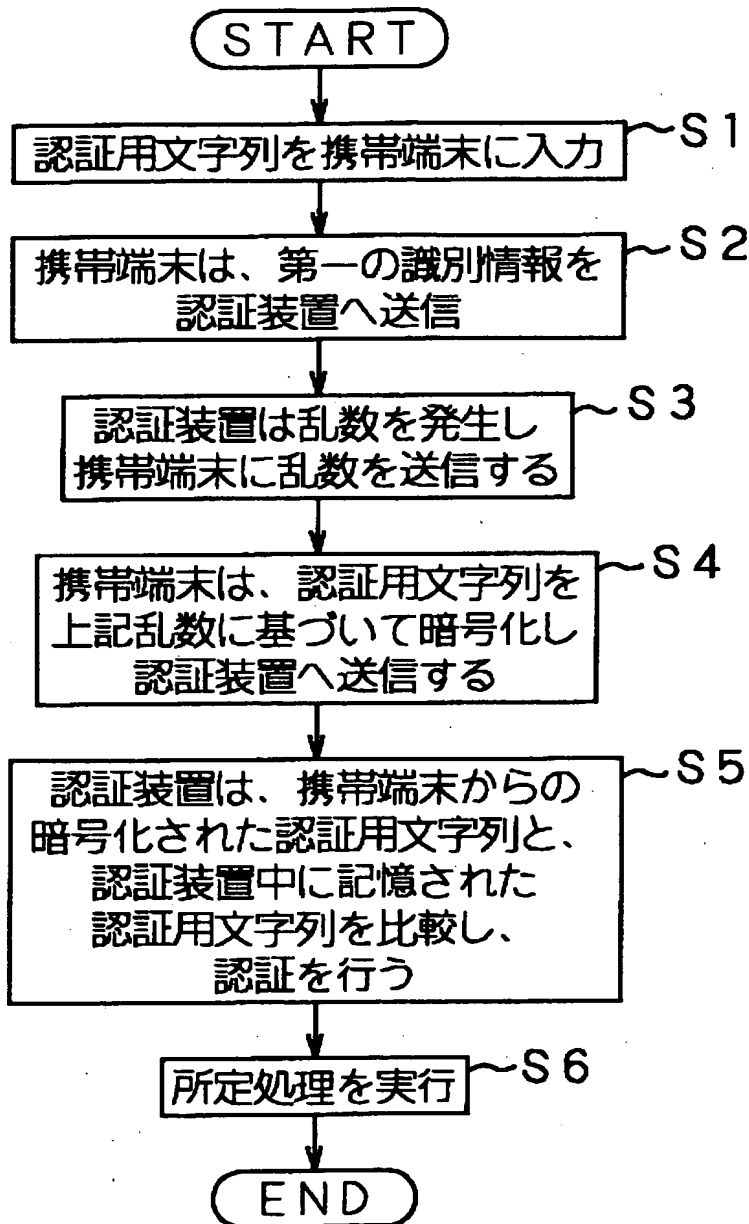
【符号の説明】

1 認証システム、10 カード、11 I D 用メモリ、12 入力部、13

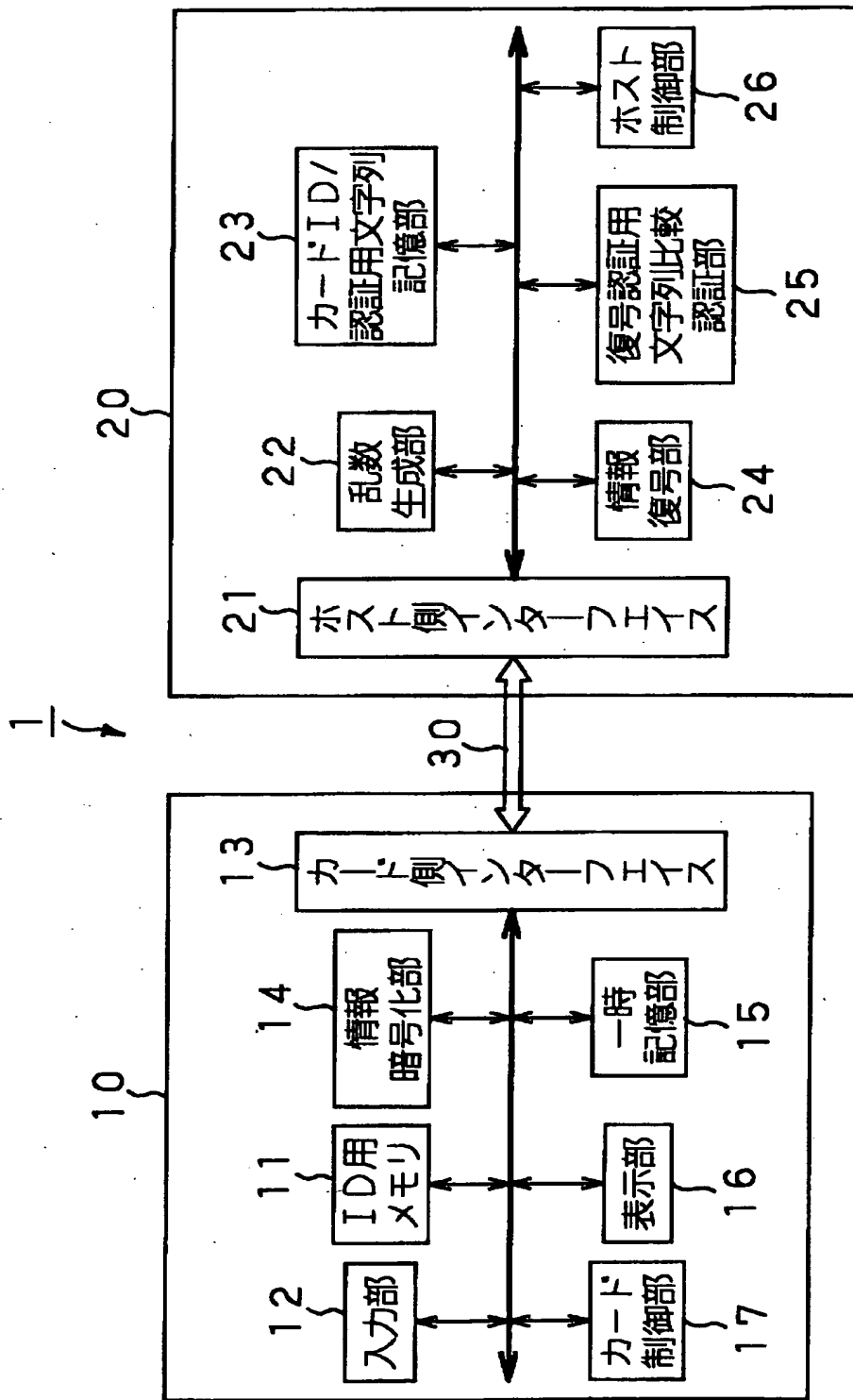
カード側インターフェイス、14 情報暗号化部、15 一時記憶部、16
表示部、17 カード制御部、20 ホストコンピュータ、21 ホスト側イン
ターフェイス、22 乱数生成部、23 カードID／認証用文字列記憶部、2
4 情報復号部、25 復号認証用文字列比較認証部、26 ホスト制御部、2
7 ホスト側情報暗号化部、28 暗号認証用情報文字列比較認証部

【書類名】 図面

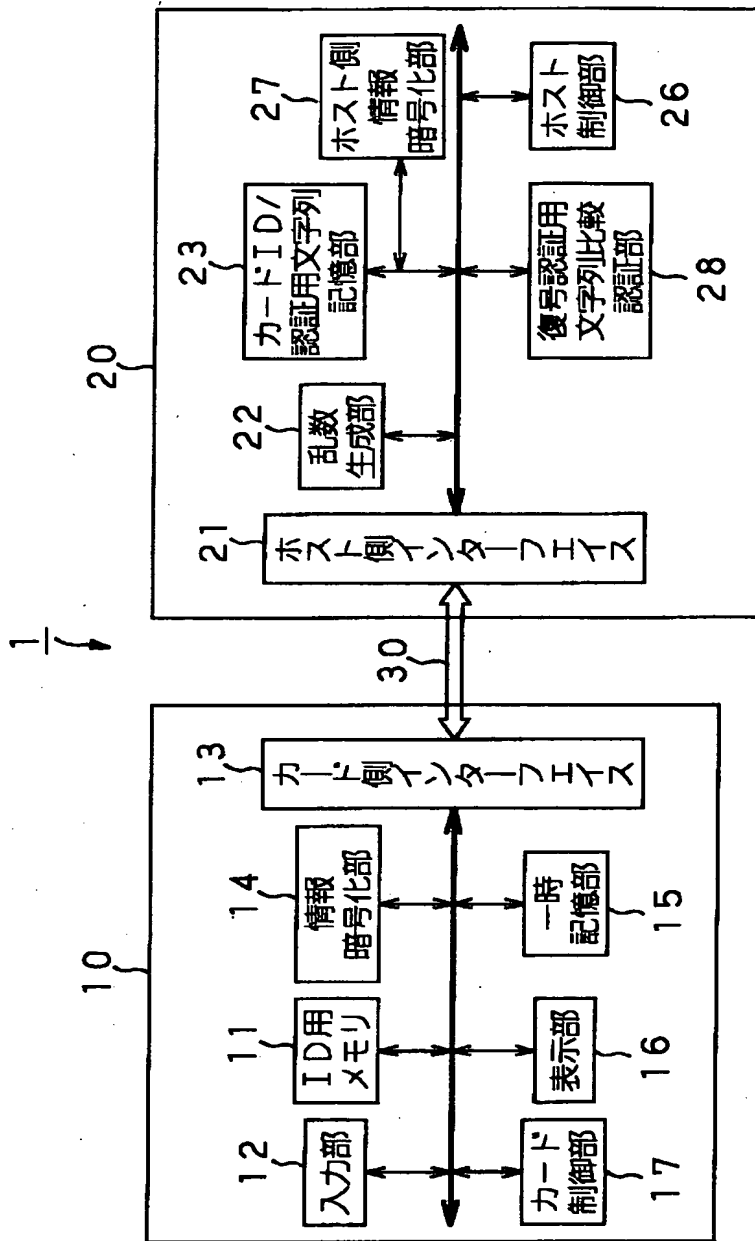
【図 1】



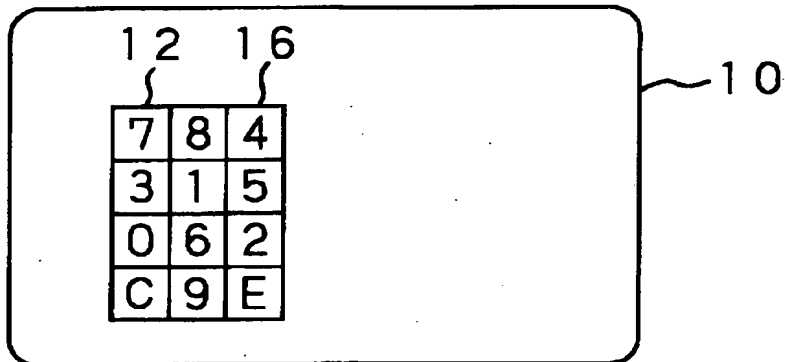
【図2】



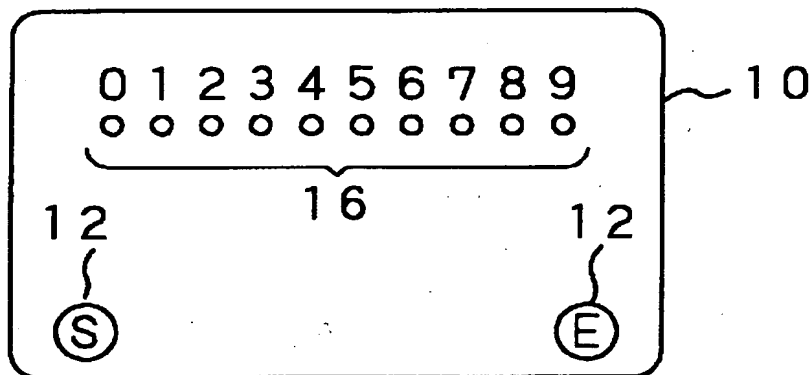
【図3】



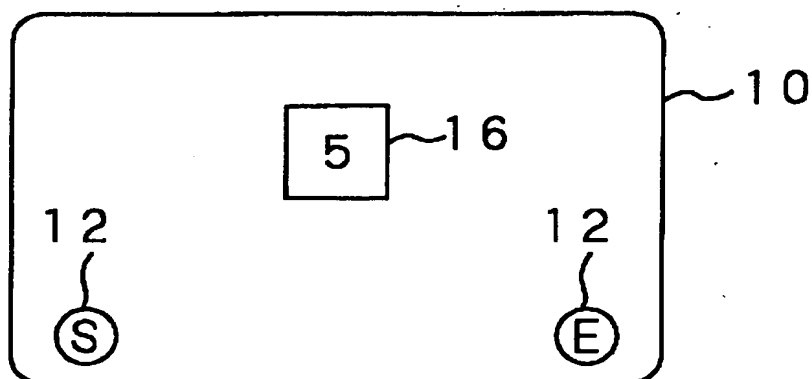
【図 4】



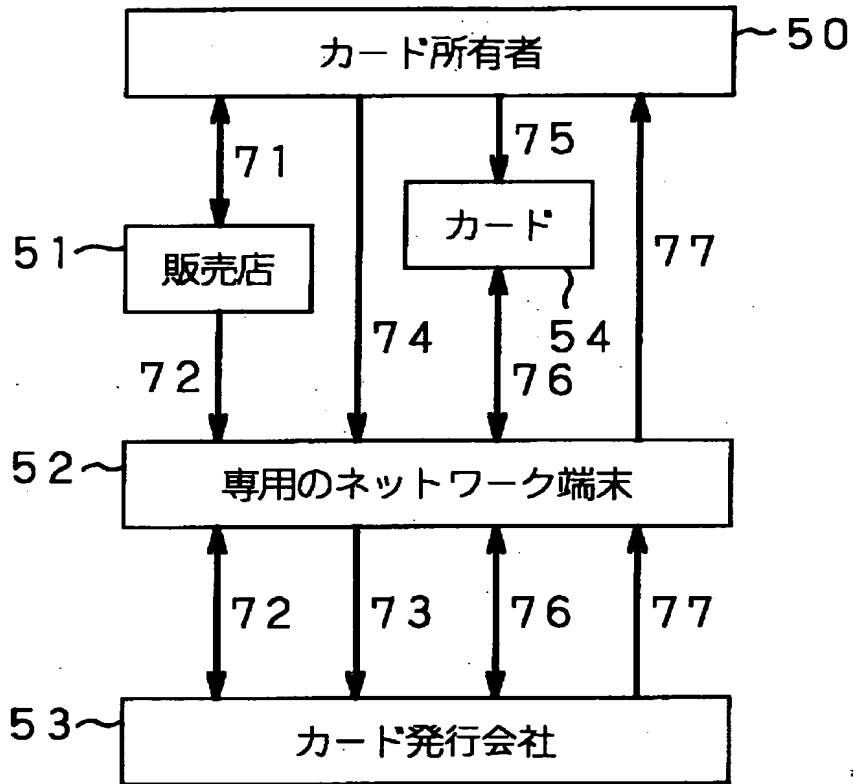
【図 5】



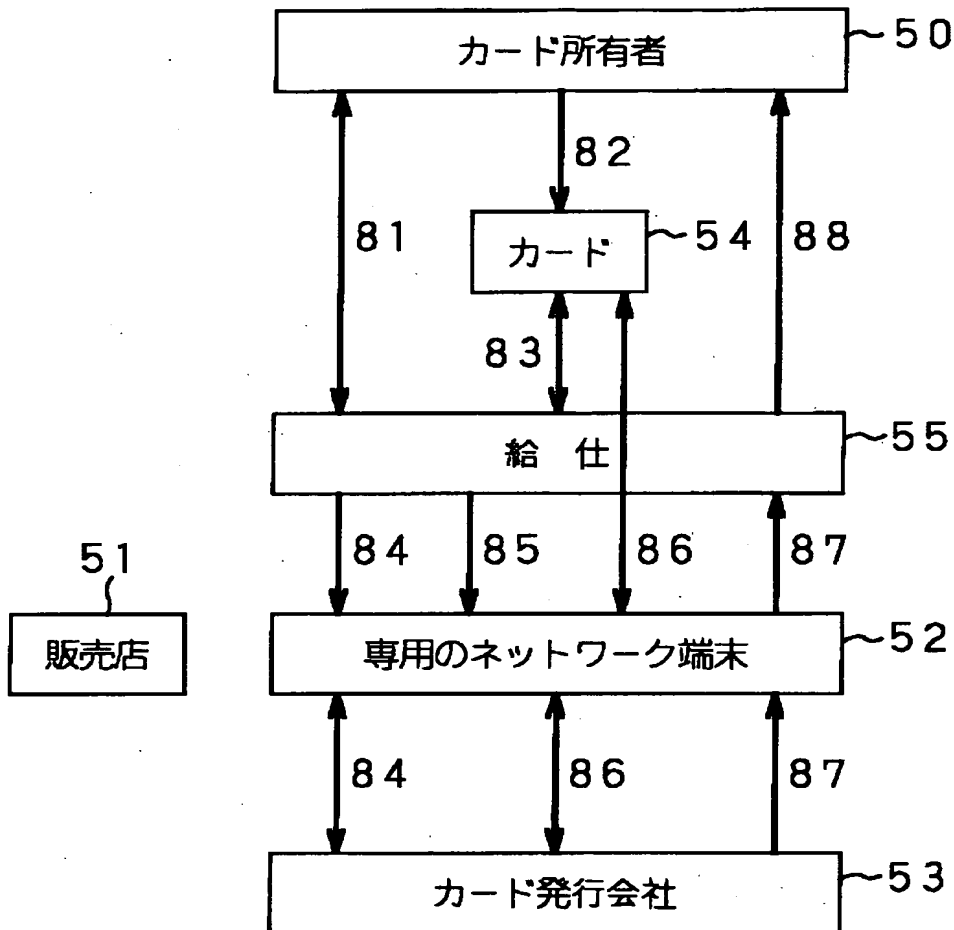
【図 6】



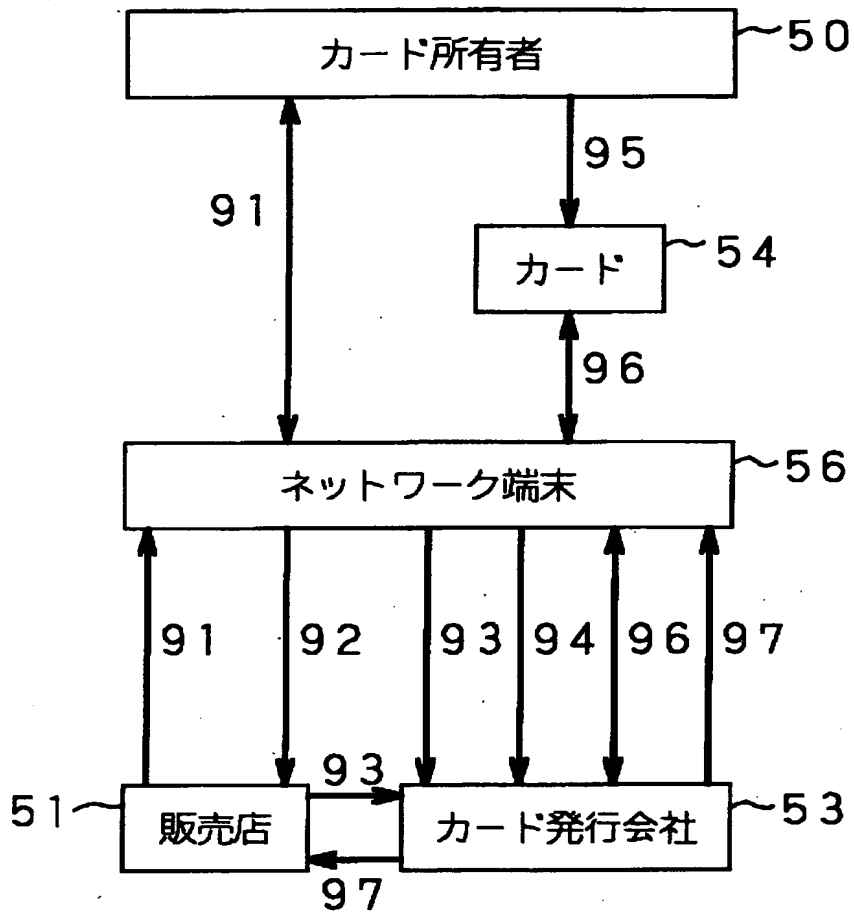
【図 7】



【図 8】



【図9】



【書類名】 要約書

【要約】

【課題】 サービスの提供者が利用者を認証するまでの過程において、第三者が個人情報をも不正に取得することを困難にする。

【解決手段】 カード10とホストコンピュータ20とが接続線30で接続されて構成される認証システムにおいて、カード10は、カードIDを記憶するID用メモリ11と、暗証番号入力等が行われる入力部12と、ホストコンピュータ20と接続されるカード側インターフェイス13と、ホストコンピュータ20から送られ、送信される毎に固有の値を有する乱数と該カードの暗証番号とを混合して符号化し認証用情報を生成する情報暗号化部14と、情報暗号化部14によって得られた認証用情報を一時的に記憶する一時記憶部15とを備える。

【選択図】 図2

出 願 人 履 歴 情 報

識別番号 [000002185]

1. 変更年月日 1990年 8月30日
[変更理由] 新規登録
住 所 東京都品川区北品川6丁目7番35号
氏 名 ソニー株式会社